

TML

DECLASSIFIED

AUG 10 2000

mmd
8/10

BANNER & WITCOFF LTD.

REVIEWED



Robert B. Levy
Senior Attorney

August 9, 2000

Joseph P. Krause, Esq.
Banner & Witcoff

RE: IDS No. 2000-0020 (DeCaluwe et al.) 87272

Please see our comments on the above-referenced
application. Thank you.

Bob Levy

Attachment

Room 3252G2
295 North Maple Avenue
Basking Ridge, NJ 07920
Tele: 908-221-5714 Fax 908-953-8360 / 908-221-5783
e-mail: rblevy@lga.att.com

AT&T
IDS 2000-0020
DeCaluwe
July 17, 2000

Serial Number 09/703,699
Declarations under 1.131
Attachment E
Page 2 of 12

METHOD FOR TRACKING SOURCE AND DESTINATION INTERNET

PROTOCOL DATA

FIELD OF THE INVENTION

This invention relates to data networks. In particular this invention relates to a
5 method and an apparatus for managing data flow in an Internet Protocol (IP) network so
as to prevent network disruption caused by excessive data flow through one or more
switches.

BACKGROUND OF THE INVENTION

Figure 1 depicts a simplified block diagram of a simplified IP data network 100 of
10 the prior art. The IP network 100 allows IP data to be sent between network users 120
and 122. A network of IP routers 102, 104, 106, and 108 (the purpose, function and
operation of which are well known in the art) are interconnected by several data paths
110, 112, 114, 116, and 118 such that data from a particular customer 120 can be routed
to/from other internet protocol data network customer 122 using any pathway through the
15 network 100 such as coaxial cable, fiber optic cable, microwave data or other appropriate
links between the routers.

As an example of a pathway through the network, data from a customer 120 might
be received at a first router 108 and routed over a data path 118 to another router 102
which routes the traffic over the pathway 110 to the other router 104 connected to the
20 destination address, customer 122. Alternate pathways through the network 100 might

AT&T
IDS 2000-0020
DeCaluwe
July 17, 2000

Serial Number 09/703,699
Declarations under 1.131
Attachment E
Page 3 of 12

route data from router 108 through router 102 to router 106 and then to router 104. Yet another pathway might exist from router 108 to 106 to 104.

A problem with an IP data network, such as the simplified depiction in Figure 1, is that one or more individual routers or internet protocol data switches can become over-
5 loaded by the transmission of data to a particular destination address or the receipt of too much data from a particular source address. Some individuals consider the generation of spurious data, thereby overloading a router, to be a prank. Curtailing such traffic might help limit the damage caused by such criminal conduct.

✓ (OR
MAKE
IT
ONE
WORD)

WHILE TRUE,
IS THIS
APPROPRIATE
IN A PATENT
APPLICATION?

It is well known that IP data packets include both source and destination
10 addresses, which are numerical indicators of the computer of the network from which the data originated and to which a packet is to be sent. In an internet protocol data system, misdelivered or discarded data packets that are not received by the destination, are
retransmitted by the source at the request of the destination when expected data packets,
do not arrive by other identifying data transmitted with each packet,

15 A problem with prior art internet protocol data switching networks is the inability to manage or control the flow of data from a particular source address or to a destination address in order to avoid overloading one or more routers in a network so as to insure the smooth flow of data packets through the overall network. A method and apparatus by which an internet protocol data network can manage the receipt of data from or to an
20 address location would be an improvement over the prior art, by at least providing a method and apparatus to control or limit damage caused by sabotage.

SEE ABOVE

{ IF THE INVENTION IS TO
MINIMIZE DAMAGE BY
HACKERS, IN PARTICULAR, THEN
STATE IT }

AT&T
IDS 2000-0020
DeCaluwe
July 17, 2000

Serial Number 09/703,699
Declarations under 1.131
Attachment E
Page 4 of 12

SUMMARY OF THE INVENTION

In an IP data network, source and destination IP addresses are recorded in memory in a router. The data on source and destination addresses of the data packets passing through the router are read through a user interface, or alternatively by a computer, to tabulate the amount of data from and to individual IP source and destination addresses.

When the data traffic from or to a particular IP address exceeds a predetermined threshold rate, the router can be controlled to discard messages either from a particular IP address or to a particular IP address via a user interface.

10 BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a simplified block diagram of a prior art internet protocol data network.

Figure 2 shows a simplified block diagram of an exemplary router device with incoming data lines, outgoing data lines and buffer and memory devices by which source and destination IP addresses are tracked and recorded.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Figure 2 shows a simplified block diagram of an improved internet protocol router 200. Incoming data lines 202, 204, and 206 carry internet protocol data packets, not shown, into the router 200; outgoing data lines 210, 212, 214 carry internet protocol (IP) data packets out of the router 200.

AT&T
IDS 2000-0020
DeCaluwe
July 17, 2000

Serial Number 09/703,699
Declarations under 1.131
Attachment E
Page 5 of 12

As is well known to those skilled in the art, IP data packets resemble Ethernet data packets in that each includes an address known as a source address that identifies a computer from which the data packet was originated. Each IP data packet also includes a destination address, which uniquely identifies the destination or end point to which the data packet is to be routed and delivered.

In Figure 2, incoming data packets, i.e., data packets arriving on incoming lines 202, 204, or 206, are received at one or more data buffers 208 within the router 200. The data buffers 208 are typically comprised of random access memory (RAM) or equivalent (perhaps an appropriate fast disk drive) and provide an elastic storage for the data packets in the router device 200 ^{THAT} but are eventually transmitted on outbound data lines 210, 212, and 214 to other points in the IP network.

While IP data packets are resident in the buffer 208 of the router 200, the source and destination IP addresses within each data packet, are copied into or stored into a memory device 216, which acts to accumulate a record of the data traffic through the router 200 over a finite period of time. By using the accumulated data in the memory device 216, a processor, either within the router 200 or outside the router via a user interface 220, tabulates or counts the occurrence of either or both the source addresses and destination addresses of data packets passing through the router 200.

By counting the occurrences of source addresses and/or destination addresses carried through the router 200 over a predetermined time interval, the length of which is a design choice, it is possible to measure the amount of traffic to and/or from a particular IP

AT&T
IDS 2000-0020
DeCaluwe
July 17, 2000

Serial Number 09/703,699
Declarations under 1.131
Attachment E
Page 6 of 12

address so as to prevent data from a particular router, such as the routers 102, 104, 106 or 108 in Figure 1, from overloading another router in the network.

By way of example, so-called computer hackers, intent on frustrating a computer network, might cause massive amounts of spurious data to be generated to or from one or more other routers in the network. Large numbers of data transmission from one switch (or source address) to another switch (or destination address) are frequently caused by deliberate acts of sabotage. (In most instances, hackers cause many switches to send data to one switch to drive it into overload) By tracking the data origins and destinations by source and destination addresses, it is possible to prevent such acts from crippling an entire data network if overruns (sometimes referred to as storms of data or data storms) of data are discarded or suppressed.

In Figure 2, a user interface 220, which provides access to the data stored in memory 216, allows the accumulated tally of source addresses and destination addresses to be manually read. If the count of source and destination addresses per unit time exceeds some predetermined threshold, commands entered by the user interface 220 configure the router 200 to ignore IP data packets from, or to, ^{the} problematic address.

In an alternate embodiment, data traffic volume to or from a particular source address is monitored automatically. In the unlikely event that the source switching system were to be sabotaged so as to generate an overwhelming amount of data for a destination address, an intervening router can inhibit the sabotaged switch from bringing a network down by overloading one or more of the intermediate nodes of the network.

AT&T
IDS 2000-0020
DeCaluwe
July 17, 2000

Serial Number 09/703,699
Declarations under 1.131
Attachment E
Page 7 of 12

In the preferred embodiment, a running count (or tabulation) of data packets received from a source address or to be sent to a destination address can be entered via the user interface 220 to the router itself 200. Alternate embodiments would certainly include substituting a computer manager ~~could be substituted~~ for the user interface 220
5 such that the computer manager 220 would automatically poll the memory 216 over time to monitor the rate at which packets are flowing through the router. In the event the data from a particular address or to another address ~~exceeding~~^{exceeded} some ~~empirically~~^{pre} determined threshold, determined either empirically or heuristically, network sabotage might be avoided by automatically suppressing the reception of additional data packets from a
10 particular source or automatically discarding data packets accordingly.

The action of discarding a data packet can be accomplished simply by ignoring incoming data packets from a source address. Alternative methods would include overriding previously stored data packets in a buffer with newly received data packets such that the end result is that the total volume of data packets from a source does not
15 exceed some predetermined allowable threshold. One or ~~messages~~^{more} might be sent from one router to another, instructing the other switch to discard packets from a particular source. A variant of such an embodiment would include sending such an alarm message throughout the network so that all switches connected therein would discard problematic data. As for the inhibition of packet transmission, an overwhelmingly large number of
20 data packets addressed to a destination^q can be controlled simply by deleting or overriding outbound packets with new or other information.

AT&T
IDS 2000-0020
DeCaluwe
July 17, 2000

Serial Number 09/703,699
Declarations under 1.131
Attachment E
Page 8 of 12

By monitoring the source address data and the destination address data in an IP protocol network, acts of sabotage on a network might be avoided. By automating the monitoring and maintenance of data traffic through the network, overall system reliability can be increased.

5

AT&T
IDS 2000-0020
DeCaluwe
July 17, 2000

Serial Number 09/703,699
Declarations under 1.131
Attachment E
Page 9 of 12

We claim:

- 1 1. In an Internet Protocol (IP) data network comprised of a plurality of
2 interconnected IP data switching systems, a method comprised of:
3 a. receiving at a first IP data switching system a plurality of IP data packets;
4 b. tabulating at said first IP data switching system at least the number of IP
5 data packets received from a particular IP source address during a first
6 time interval thereby forming a count of IP data packets from a particular
7 source;
8 c. storing said count of IP data packets in a memory device for subsequent
9 processing.

- 1 2. The method of claim 1 further including the step of:
2 d. reading said count of IP data packets from said memory device;
3 e. selectively discarding IP data packets received at said first IP data
4 switching system that originated ^{WHAT?}

WHAT
TRIGGERS
THE
DISCARD?

- 1 3. The method of claim 1 wherein said IP data switching system is an IP data
2 router switching system.

AT&T
IDS 2000-0020
DeCaluwe
July 17, 2000

Serial Number 09/703,699
Declarations under 1.131
Attachment E
Page 10 of 12

WHAT
TRIGGERS
THE
DENIAL?

1 4. The method of claim 2 wherein said step of selectively discarding IP data
2 packets includes the step of denying reception of IP data packets from a router
3 based upon a source address in IP data packets.

1 5. In an Internet Protocol (IP) data network comprised of a plurality of
2 interconnected IP data switching systems, a method comprised of:
3 a. sending a plurality of IP data packets from a first IP data switching system
4 to a second IP data switching system;
5 b. tabulating at said first IP data switching system at least the number of IP
6 data packets sent to a particular IP destination address during a first time
7 interval, thereby forming a count of IP data packets sent to a particular IP
8 destination address;
9 c. storing said count of IP data packets sent to a particular IP destination
10 address in a memory device for subsequent processing.

✓

1 6. The method of claim 5 further including the step of:
2 d. reading said count of IP data packets from said memory device;
3 e. selectively inhibiting the transmission of IP data packets from said first
4 ~~said first~~ IP data switching system to said second IP data switching
5 system.

SEE
QUESTION
ABOVE

✓

AT&T
IDS 2000-0020
DeCaluwe
July 17, 2000

Serial Number 09/703,699
Declarations under 1.131
Attachment E
Page 11 of 12

1 7. The method of claim 5 wherein at least one of said first and second IP data
2 switching systems is an IP data router switching system.

1 8. The method of claim 5 wherein said step of selectively inhibiting the
2 transmission of IP data packets includes the step of sending a message to a
3 specific router to discard messages either received from or sent to a specific IP
4 address.

AT&T
IDS 2000-0020
DeCaluwe
July 17, 2000

Serial Number 09/703,699
Declarations under 1.131
Attachment E
Page 12 of 12

ABSTRACT OF THE DISCLOSURE

In an IP network, tabulating the number of data packets received from and/or sent to a particular IP address over time can provide a mechanism by which it is possible to determine or predict overloading^{of} a node or nodes in an IP data network. By selectively deleting data packets received from a suspect source address or inhibiting the transmission of data packets to a suspect destination address, network management and control can be readily accomplished. ✓

5